

# EC386 Cryptography & Data Security

*Arulalan Rajan*

*Formerly, Dept. of E&C Engg, NITK Surathkal*

*Lecture - 1, 23 July 2018*

*Introduction*

# Cryptograph(Y)?

# Cryptograph(Y)?

- Careful storage of sensitive information

# Cryptograph(Y)?


- Careful storage of sensitive information
- Transmission of sensitive information over insecure channel

# Cryptograph(Y)?


- Careful storage of sensitive information
- Transmission of sensitive information over insecure channel
- *Science of secret writing with the goal of hiding the meaning of a message!*



# Cryptograph(Y)?

- Careful storage of sensitive information
- Transmission of sensitive information over insecure channel
- *Science of secret writing with the goal of hiding the meaning of a message!*  

- Wouldn't want any TDH to read the message that is meant for my friend!

# Cryptograph(Y)?



- Careful storage of sensitive information
- Transmission of sensitive information over insecure channel
- *Science of secret writing with the goal of hiding the meaning of a message!*  

- Wouldn't want any TDH to read the message that is meant for my friend!

What will happen if my prof knows what am commenting about him or her during lectures?

Oooooooooohhhh

Mannnnnn!!!!  

# Cryptograph(Y)?

- Careful storage of sensitive information
- Transmission of sensitive information over insecure channel
- *Science of secret writing with the goal of hiding the meaning of a message!*  

- Wouldn't want any TDH to read the message that is meant for my friend!
- After all you are used to this elsewhere !!! 



What will happen if my prof knows what am commenting about him or her during lectures?

Oooooooooohhhh

Mannnnnn!!!!  




# Cryptograph(Y)?

- Careful storage of sensitive information
- Transmission of sensitive information over insecure channel
- *Science of secret writing with the goal of hiding the meaning of a message!*  

- Wouldn't want any TDH to read the message that is meant for my friend!
- After all you are used to this elsewhere !!! 

What will happen if my prof knows what am commenting about him or her during lectures?



Oooooooooohhhh

Mannnnnn!!!!  

Worst case, Prof may get bugged and still give marks for the encryption i do in my answer sheet! 

# Cryptograph(Y)?


## Confidentiality & Privacy Goals

- Careful storage of sensitive information
- Transmission of sensitive information over insecure channel
- *Science of secret writing with the goal of hiding the meaning of a message!*  

- Wouldn't want any TDH to read the message that is meant for my friend!
- After all you are used to this elsewhere !!! 

What will happen if my prof knows what am commenting about him or her during lectures?

Oooooooooohhhh

Mannnnnn!!!!  

Worst case, Prof may get bugged and still give marks for the encryption i do in my answer sheet! 

# Cryptography - What?

# Cryptography - What?

- Use Math to encrypt and decrypt data

# Cryptography - What?

- Use Math to encrypt and decrypt data
- Means what? 🤔

# Cryptography - What?

- Use Math to encrypt and decrypt data
- Means what? 🤔
- Disguise message into some other garbled one!!!

# Cryptography - What?

- Use Math to encrypt and decrypt data
- Means what? 🤔
- Disguise message into some other garbled one!!!
- Any non-math way of disguising messages? 🤔

# Cryptography - What?

- Use Math to encrypt and decrypt data
- Means what? 🤔
- Disguise message into some other garbled one!!!
- Any non-math way of disguising messages? 🤔
- You know it! 😂



# Cryptography - What?

- Use Math to encrypt and decrypt data
- Means what? 🤔
- Disguise message into some other garbled one!!!
- Any non-math way of disguising messages? 🤔
- You know it! 😂
- How do we do this disguising?

# Cryptography - What?

- Use Math to encrypt and decrypt data
- Means what? 🤔
- Disguise message into some other garbled one!!!
- Any non-math way of disguising messages? 🤔
- You know it! 😂
- How do we do this disguising?

**Unintelligible to the Unauthorized**

# Cryptography - How?

# Cryptography - How?

- Simple substitution of one character for the other

# Cryptography - How?

- Simple substitution of one character for the other
- Reordering or scrambling of data

# Cryptography - How?

- Simple substitution of one character for the other
- Reordering or scrambling of data
- Advanced techniques using special keys

# Cryptography - How?

- Simple substitution of one character for the other
- Reordering or scrambling of data
- Advanced techniques using special keys
- and a lot more ...

# Some *Formal* Definitions



# Some *Formal* Definitions

- ***Plaintext:*** *In the most jargonized form, the information to be concealed*

# Some *Formal* Definitions

- ***Plaintext:*** *In the most jargonized form, the information to be concealed*
- *In layman terms, Plaintext - Message!*

# Some *Formal* Definitions

- ***Plaintext:*** *In the most jargonized form, the information to be concealed*
- *In layman terms, Plaintext - Message!*
- ***Encryption / Enciphering:*** *Operation of disguising plaintext to hide its substance*

# Some *Formal* Definitions

- ***Plaintext:*** *In the most jargonized form, the information to be concealed*
- *In layman terms, Plaintext - Message!*
- ***Encryption / Enciphering:*** *Operation of disguising plaintext to hide its substance*
- ***Ciphertext / Cryptogram:*** *Enciphered Plaintext*

# Some *Formal* Definitions

- ***Plaintext***: *In the most jargonized form, the information to be concealed*
- *In layman terms, Plaintext - Message!*
- ***Encryption / Enciphering***: *Operation of disguising plaintext to hide its substance*
- ***Ciphertext / Cryptogram***: *Enciphered Plaintext*
- ***Recipient / Receiver***: *Authorized person to whom the cryptogram is sent!*

# Some *Formal* Definitions

# Some *Formal* Definitions

- **Algorithm:** *Set of rules the encipherer uses to encipher his message!*

# Some *Formal* Definitions

- **Algorithm:** *Set of rules the encipherer uses to encipher his message!*
- **Key:** *Password to encrypt as well as decrypt the plaintext uniquely*



# Some *Formal* Definitions

- **Algorithm:** *Set of rules the encipherer uses to encipher his message!*
- **Key:** *Password to encrypt as well as decrypt the plaintext uniquely*
- **Deciphering / Decryption:** *Applying key to translate back from the ciphertext to plaintext*

# Some *Formal* Definitions

- **Algorithm:** *Set of rules the encipherer uses to encipher his message!*
- **Key:** *Password to encrypt as well as decrypt the plaintext uniquely*
- **Deciphering / Decryption:** *Applying key to translate back from the ciphertext to plaintext*
- **Code:** *System that does not depend on key or has only one possible key - Ex: Morse Code!*

# Some *Formal* Definitions

Sirrrr!!! That's the limit! 😡

Don't tell us you are gonna define what an algorithm is!!!

- **Algorithm:** Set of rules the encoder uses to transform his message!
- **Key:** Password to encrypt as well as decrypt the plaintext *uniquely*
- **Deciphering / Decryption:** Applying key to translate back from the ciphertext to plaintext
- **Code:** System that does not depend on key or has only one possible key - *Ex: Morse Code!*

# Some *Formal* Definitions

# Some *Formal* Definitions

- ***Interceptor***: Someone who intercepts message from encipherer to the recipient, has no knowledge of the key

# Some *Formal* Definitions

- ***Interceptor***: Someone who intercepts message from encipherer to the recipient, has no knowledge of the key
- ***Cryptography***: Design of Cipher Systems

# Some *Formal* Definitions

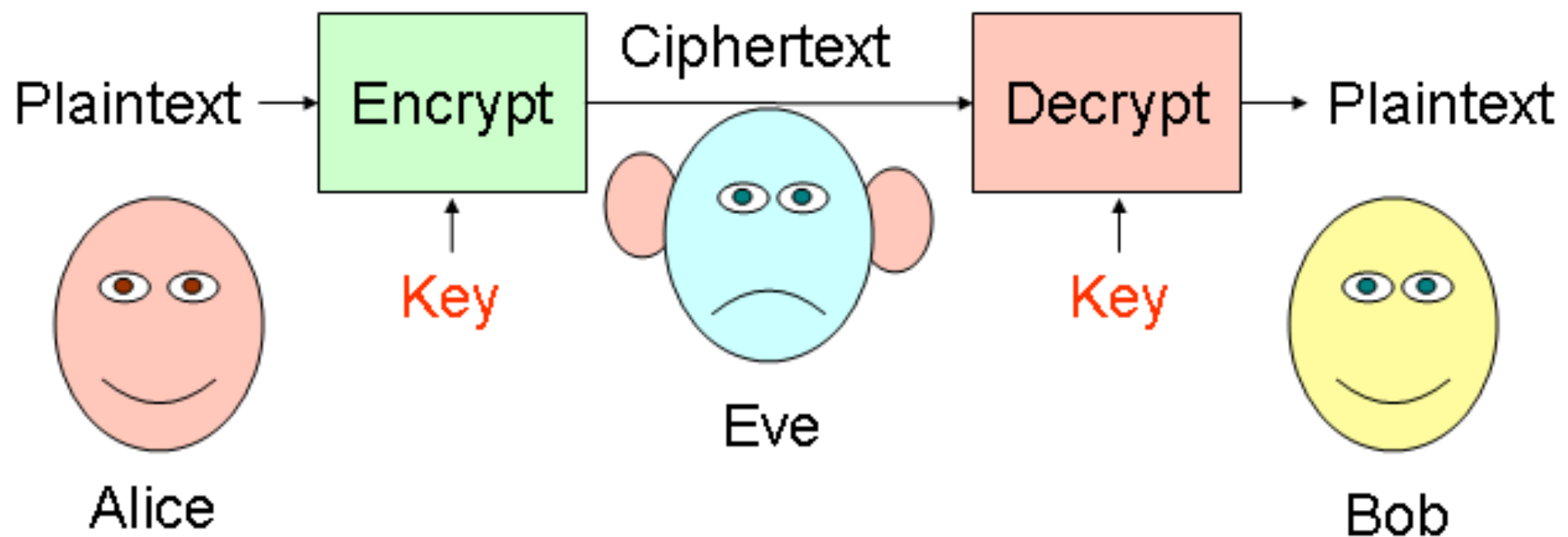
- **Interceptor:** *Someone who intercepts message from encipherer to the recipient, has no knowledge of the key*
- **Cryptography:** *Design of Cipher Systems*
- **Cryptanalysis:** *Process of deducing plaintext from cipher text, without the knowledge of the key... Probably even the key!*

# Some *Formal* Definitions

- **Interceptor:** *Someone who intercepts message from encipherer to the recipient, has no knowledge of the key*
- **Cryptography:** *Design of Cipher Systems*
- **Cryptanalysis:** *Process of deducing plaintext from cipher text, without the knowledge of the key... Probably even the key!*
- **Cryptology:** *Cryptography + Cryptanalysis*



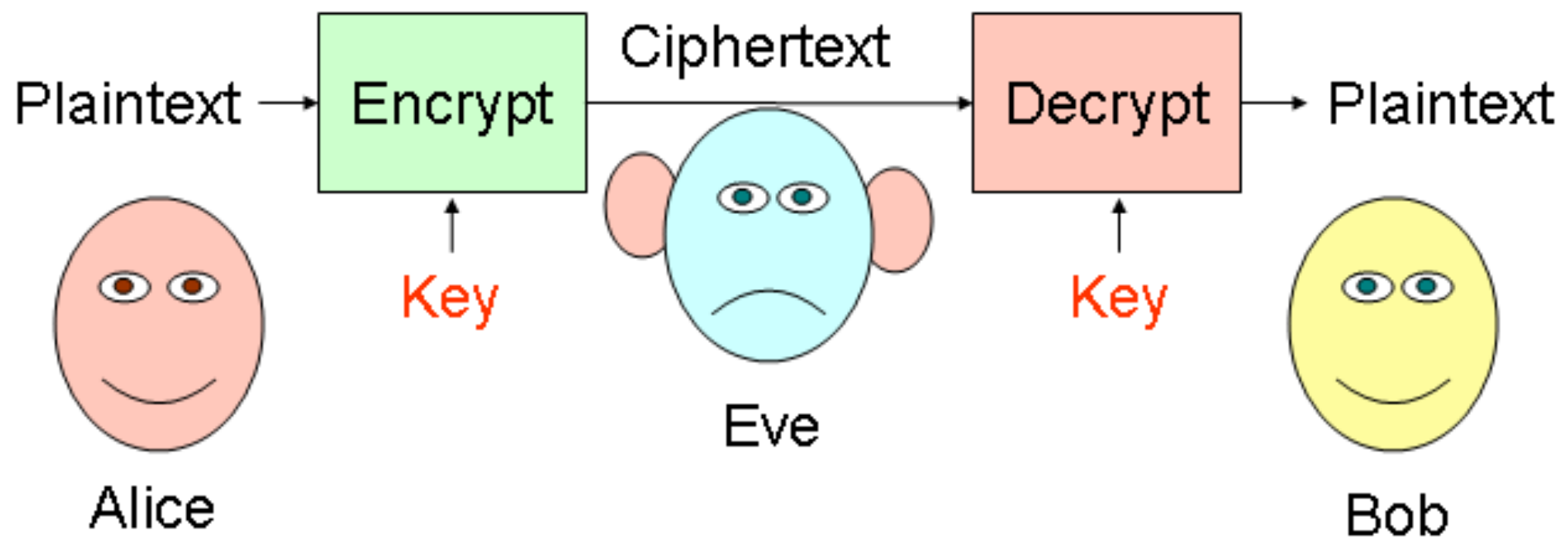
# Cipher System - Illustrated



$$\text{Ciphertext} = \text{Encrypt}(\text{Plaintext}, \text{Key})$$
$$\text{Plaintext} = \text{Decrypt}(\text{Ciphertext}, \text{Key})$$

# Cipher System - Illustrated

Shabbbbaaaaa!!! Some non text  
slide after a long time!!! 🙄



$$\text{Ciphertext} = \text{Encrypt}(\text{Plaintext}, \text{Key})$$
$$\text{Plaintext} = \text{Decrypt}(\text{Ciphertext}, \text{Key})$$

# Security Requirements of a communication system

# Security Requirements of a communication system

- *Authentication: Process of proving one's identity*

# Security Requirements of a communication system

- **Authentication:** *Process of proving one's identity*
- **Privacy/Confidentiality:** *Ensuring no-one can read the message except the intended one*

# Security Requirements of a communication system

- **Authentication:** *Process of proving one's identity*
- **Privacy/Confidentiality:** *Ensuring no-one can read the message except the intended one*
- **Integrity:** *Assuring the receiver that the message was not altered in anyway from the original*

# Security Requirements of a communication system

- **Authentication:** *Process of proving one's identity*
- **Privacy/Confidentiality:** *Ensuring no-one can read the message except the intended one*
- **Integrity:** *Assuring the receiver that the message was not altered in anyway from the original*
- **Non-Repudiation:** *Mechanism to prove that the sender has indeed sent the message!*

# Security Requirements of a communication system

- **Authentication:** *Process of proving one's identity*
- **Privacy/Confidentiality:** *Ensuring no-one can read the message except the intended one*
- **Integrity:** *Assuring the receiver that the message was not altered in anyway from the original*
- **Non-Repudiation:** *Mechanism to prove that the sender has indeed sent the message!*
- *In simple terms, non repudiation - Ability to prevent denial*



On a lighter note,

On a lighter note,

*There are two kinds of cryptography in this world - The one that prevents your kid sister from reading your files and the other that stops the government from reading your files!*

On a lighter note,

*There are two kinds of cryptography in this world - The one that prevents your kid sister from reading your files and the other that stops the government from reading your files!*

*- Bruce Schneier*